ExtraHop Addy: Security Overview

Secure Machine Learning in the Cloud

ExtraHop takes the security of your data very seriously. The cloud-based Addy machine learning service is designed to keep your data secure. This document provides an overview of how Addy works and explains what types of data are sent to the cloud.

Why Addy Is Important

Machine learning to detect real issues faster

In today's world of big data, IT organizations are often overwhelmed with information and do not have enough skilled staff to interpret it. As a result, performance and security issues go unheeded until someone notices, resulting in lost revenue, poor customer experiences, or security incidents. Even worse, some issues go unnoticed entirely. ExtraHop, the leader in real-time IT analytics, has developed Addy, a machine learning service, to assist IT and security teams in identifying and resolving issues faster.

Architecture Overview

On-premises processing with cloud-based computing resources

Addy is unlike a typical SaaS solution. Only high-level IT metrics are sent to Addy in the cloud. The Addy service does not ingest payloads, filenames, strings, or other data categories that could contain sensitive data. This design enables the ExtraHop solution to apply machine learning across a large data set while keeping the most sensitive data categories on-premises under the control of customer. ExtraHop has received SOC 2, Type 1 compliance certification for the Addy service.

Addy uses a mix of on-premises technology and cloud services, as illustrated below.

1. The ExtraHop Discover Appliance (EDA) is an on-premises device that remains in the customer's custody and control. It analyzes network traffic to extract 4,500+ metrics, which are stored on the appliance. These metrics include IP addresses, URIs, database queries, CIFS filenames, VoIP phone numbers, and other data that may be considered sensitive. Customers can configure the EDA to collect custom metrics that may contain additional data.

2. When Addy is enabled, the EDA sends a subset of its metrics to a customer-dedicated cloud-computing instance in Amazon Web Services, which is operated by ExtraHop. Other than IP addresses, the metrics sent to Addy do not include any data that may be considered protected health information or personally identifiable information. For example, the number or count of files written is a metric that would be sent to Addy, but not the filenames. No custom metrics are sent to Addy.

3. The Addy service uses the metrics to build activity baselines for devices, networks, and applications. When activity deviates from those baselines, an anomaly event is sent back to the EDA. Customers may also opt-in to receive email alerts when an anomaly is detected. These email messages also do not include sensitive data.